REMARKS

Claims 1, 3-7, 9, 10, 17, and 21-31 are pending in the present application. By this Response, claims 1 and 17 are amended, claims 16 and 18-20 are canceled, and claims 28-31 are added. Claims 1 and 17 are amended to clarify that the authentication credential container is part of the data processing system and that the credential information is received from the separate hardware device into this authentication credential container of the data processing system. Claims 28-31 are added to recite computer program product versions of claims 1, 3, 4, and one or more of claims 21-27. No new matter has been added by the above amendments to the claims or addition of new claims. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Telephone Interview

Applicant thanks Examiner Johnson for the courtesies extended to Applicant's representative during the July 8, 2009 telephone interview. During the telephone interview, the above amendments and the distinctions of the claims over the cited art were discussed. Examiner Johnson acknowledged that he understood Applicant's position with regard to the references not teaching or rendering obvious the generation of a consolidated view of authentication information for a plurality of applications from authentication information obtained from a separate hardware security device and brought into a credential container. Examiner Johnson agreed to discuss the case in detail with his primary once this Response was filed and would contact Applicant's representative if anything further was necessary to place the application in better condition for allowance. The substance of the telephone interview is summarized in the following remarks.

II.   Rejection under 35 U.S.C. § 103(a) Based on Schaeck, Delany, Cotte, and Yasuda

The Office Action rejects claims 1, 3-7, 9, 10, and 21-27 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schaeck et al. (U.S. Patent Application Publication No. 2003/0163513), in view of Delany et al. (U.S. Patent Application Publication No. 2002/0138763), Cotte (U.S. Patent Application Publication No. 2004/0013132), and further in view of Yasuda et al. (U.S. Patent No. 7,114,075). This rejection is respectfully traversed.

Independent claim 1 reads as follows:

1.   A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:
  receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user;
  identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container associated with the user;
  generating, by the data processing system, a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and
  displaying, by the data processing system, the view to the administrator.
(emphasis added)

Applicant respectfully submits that neither Schaeck, Delany, Cotte, nor Yasuda, either alone or in combination, teach or provide any technical rationale to implement at least the features emphasized above in claim 1.

Schaeck

Schaeck is directed to a mechanism for providing role based views of business web portals. With the mechanism of Schaeck, an aggregated service is comprised of one or more software resources. A role-specific portlet for each role supported by a particular one of the software resources is provided. A linkage between the role-specific portlets and the roles of the particular software resources is provided. At run time, a user role corresponding to a user of the aggregated services is obtained and a corresponding one of the role-specific portlets is programmatically selected to thereby provide a role-specific view of the aggregated service. The mechanism further determines which of the software resources to invoke to position the user's entry point into the aggregated service and uses the obtained role to select a role specific view of the determined software resource.

While Schaeck teaches to aggregate portlets for a user into an aggregate portal page view (see Figure 7 of Schaeck), nowhere in Schaeck is there any teaching or technical rational provided regarding implementing the features of "receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user" as recited in claim 1. To the contrary, in Figure 7 of Schaeck it is clearly shown that the user is presented with available services, the user selects a service, and based on the user's role, portlets associated with the service are selected and combined into an aggregate portal page that is presented to the user. Schaeck provides no teaching or technical rationale provided regarding implementing a separate hardware security device, let alone receiving credential information for each application of a plurality of applications that the user uses from the separate hardware security device in response to the separate hardware security device being coupled to a data processing system or receiving such credential information into an authentication credential container associated with the user.

Moreover, Schaeck does not teach that the view that is generated is a consolidated user directory that contains user authentication information across a plurality of applications. To the contrary, the "view" that is generated in Schaeck is a portal page that has the portlets for a selected service. There is no teaching or technical rationale

provided in Schaeck to implement this portal page such that it contains user authentication information across a plurality of applications. To the contrary, as described in paragraph [0073] of Schaeck, the portlets provide different interfaces for different user roles. In paragraph [0081] Schaeck teaches that the user's role is determined based on the user's login information, but this does not teach or provide any technical rationale to implement the actual view that is generated in Schaeck to contain user authentication information across a plurality of applications.

Cotte

Cotte does not teach or provide any technical rationale regarding implementing these features either, whether Cotte is taken alone or in combination with Schaeck. Cotte is cited as alleged teaching a plurality of applications at paragraph [0116]. Cotte is directed to a multiprotocol communications environment. In paragraph [0116] of Cotte, all that is taught is that it is possible to access a telecommunications portal in order to retrieve data about different telecommunications web sites residing on that telecommunications portal in total. There is nothing in Cotte that teaches or provides any technical rationale to implement the specific features of claim 1 discussed above with regard to Schaeck, i.e. a separate hardware device that is coupled to a data processing system; receiving, in response to a coupling of the separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user; or a view that is generated is a consolidated user directory that contains user authentication information across a plurality of applications. Merely providing a telecommunications portal that provides information about telecommunications web sites has nothing to do with identifying a plurality of applications that a user may access from a separate hardware security device in response to such a device being coupled to a data processing system or that a view that is presented is a consolidated user directory that contains user authentication information across the plurality of applications.

Delany

The Office Action admits that Shaeck does not teach a consolidated user directory (Office Action, page 5) or a complete listing of applications (Office Action, page 6). The Office Action alleges that Cotte teaches a complete listing of applications in paragraph [0116] which has been addressed above and has been shown to not actually teach or provide any technical rationale to implement such a feature but instead simply a presentation of information about telecommunications web sites. The Office Action further alleges, at pages 5-6, that Delany discloses a consolidated user directory that contains user authentication information across a plurality of applications at paragraph [0113], lines 13-18 and paragraph [0129], lines 16-20 which read as follows:

> [0113] With Group Manager 44, companies (or other entities) can allow individual users to do the following: (1) self-subscribe to and unsubscribe from groups, (2) view the groups that they are eligible to join or have joined, and (3) request subscription to groups that have access to the applications they need. Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly. Group Manager 44 also lets companies form dynamic groups specified by an LDAP filter. The ability to create and use dynamic groups is extremely valuable because it eliminates the administrative headache of continually keeping individual, static membership up-to-date. With dynamic group management features, users can be automatically added or removed if they meet the criteria specified by the LDAP filter. Dynamic groups also greatly enhance security since changes in user identities that disqualify someone from membership in a group are automatically reflected in the dynamic group membership.

> [0129] When database manager 120 starts, it will read the directory server configuration file(s) and insert corresponding profile and agent objects to its internal tables for later reference. FIG. 3 shows database manager 120 in communication with profiles 122, 124, 126 and 128. Each profile corresponds to an agent. For example, profile 122 corresponds to agent 130, profile 124 corresponds to agent 132, profile 126 corresponds to agent 134, and profile 128 corresponds to agent 136. Each agent is associated with a connection manager and a data store. For example, agent 130 is associated with connection manager 140 and data store 36a. Agent 132 is associated with connection manager 142 and data store 36b. Agent 134 is associated with connection manager 144 and data store 36c. Agent 136 is associated with connection manager 146 and data store 36d. In one embodiment, each of the data stores are LDAP directory servers with

LDAP directories. In other embodiments, one or more of the data stores are LDAP directories and one or more of the data stores are other types of data stores (e.g. SQL servers) or others. In further embodiments, none of the data stores are LDAP directories.

As discussed in Responses filed April 30, 2008 and June 18, 2008 (page 13), and the Appeal Brief filed December 4, 2008, these sections of Delany only teach that (1) with the Group Manager in Delany, a user may view the groups that they are eligible to join or have joined, view the groups that they are eligible to join or have joined, and request subscription to groups that have access to the applications they need; (2) groups may be created dynamically with an LDAP filter; (3) the database manager reads a configuration file and inserts profile and agent objects to its internal tables; (4) each profile corresponds to an agent and each agent is associated with a connection manager and a data store which may be an LDAP directory server. Nothing in these sections, or any other sections, of Delany teach or provide any technical rationale to implement generating a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications. Moreover, nothing in Delany teaches or provides any technical rationale to implement the feature of receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user.

Yasuda

The Office Action admits that the combination of Schaeck, Delany, and Cotte does not teach a separate hardware security device (see Office Action, page 6, bottom of page). However, the Office Action alleges that these features are taught by Yasuda.

Yasuda is directed to a user authentication apparatus in which an IC card is used that has authentication information for a user for a number of applications. As described in columns 6 and 7 of Yasuda, with the use of the IC card, a user supplies a PIN which is then compared, within the IC card, to a stored PIN. If the PINs match, the client computer is given access to the IC card. A list of application names stored in records of

the memory unit of the IC card is requested by the client and the names are returned by the IC card (column 6, lines 62-67). The names may be displayed to the user who then selects a name from the list (column 7, lines 1-5). In response to the user's selection, the authentication information for the selected application name is retrieved and provided to the client computer which inserts it into a logon image (column 7, lines 6-31).

While Yasuda teaches an IC card that may store authentication information for a applications accessible by a user, nowhere in Yasuda is there any teaching or technical rationale provided with regard to *credential information for each application in a plurality of applications* being received *in an authentication credential container of the data processing system* from the IC card of Yasuda. To the contrary, Yasuda only teaches providing the authentication information for a single application in response to a user selecting that single application from the list of application names provided. Yasuda does not teach an authentication credential container being provided in the client of Yasuda and does not teach that such an authentication credential container receives authentication information for a plurality of applications from a separate hardware device. All that Yasuda teaches is that authentication information for a single application is provided to the client which then inserts it into a logon image.

Moreover, nowhere in Yasuda is there any teaching or technical rationale provided to implement generating a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory *that contains user authentication information across the plurality of applications*. To the contrary, Yasuda merely teaches providing a list of application names and, in response to a user selecting a name from the list, providing the authentication information for that single application to the client such that the client may immediately insert it into a logon image. There is no view of a plurality of applications provided in Yasuda where the view contains a consolidated user directory that contains user authentication information across a plurality of applications. The listing of application names in Yasuda does not provide any view of authentication information across a plurality of applications.

Thus, for at least the reasons set forth above, Applicant respectfully submits that none of the cited references, Schaeck, Cotte, Delany, and Yasuda, whether taken alone or in combination, teaches or provides any technical rationale to implement the features of

independent claim 1. Claims 3-7, 9, 10, and 21-27 depend from claim 1 and thus, are distinguished over the alleged combination of Schaeck, Cotte, Delany, and Yasuda at least by virtue of their dependency. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1, 3-7, 9, 10, and 21-27 under 35 U.S.C. § 103(a).

In addition to the above, the alleged combination of references fails to teach or provides any technical rationale to implement the specific additional features presented in the dependent claims.

1. Dependent Claims 3 and 6

With regard to claim 3, Applicant respectfully submits that none of the cited references, whether taken alone or in combination, teaches or provides any technical rationale to implement *removing access to an application* from the plurality of the applications *by utilizing the view of the plurality of the applications accessible by the user*. Again, none of the cited references teach or provide any technical rationale to implement a view that is a consolidated user directory that contains user authentication information across the plurality of applications. Therefore, the references cannot possibly teach or provide any technical rationale to implement using such a view to remove access to an application.

The Office Action (page 8) alleges that these features are taught by Schaeck at paragraphs [0043] and [0068] with the exception of providing a complete listing of applications, which the Office Action again alleges is taught by Cotte. Paragraphs [0043] and [0068] of Schaeck only teach that a service may have a number of different views established for the service and users with particular roles are provided with different views of the service. There is nothing in these sections of Schaeck that teach or provide any technical rationale to implement anything regarding using a view that is a consolidated user directory to remove access to an application, as recited in claim 3. Moreover, none of the other cited references teach or provide any technical rationale to implement such features.

Since the cited references do not teach or provide any technical rationale to implement the features of claim 3 as noted above, the cited references further cannot teach or provide any technical rationale to implement the features of claim 6, with regard

to the removing being performed automatically, at least by virtue of the dependency of claim 6 from claim 3.

2. Dependent Claims 4, 5, and 7

Regarding claim 4, Applicant respectfully submits that none of the cited references, whether taken alone or in combination, teach or provide any technical rationale to implement creating a user account for a new application to be accessible by the user utilizing the generated view or injecting authentication information of the user account into the authentication credential container of the user. The Office Action (pages 8-11) again alleges that the view feature is taught by Schaeck at paragraphs [0043] and [0068], which have been addressed above. The Office Action further references paragraph [0052] of Schaeck which only teaches that a composition tool may be used to combine fine grain services with a larger more general service. This does not provide any further teaching or technical rationale relevant to the view feature of the claims.

With regard to the features of creating a user account for a new application using the view and injecting authentication information of the user account, the Office Action points to Delany, paragraphs [0108] and [0109] as allegedly teaching these features. While these paragraphs do mention the creation and deletion functions of user management, there is no teaching or technical rationale provided in Delany regarding implementing the specific feature of using a view that is a consolidated user directory that contains user authentication information across a plurality of applications to perform such creation or deletion or injecting authentication information into an authentication credential container of the user.

Since the cited references do not teach or provide any technical rationale to implement the features of claim 4 as noted above, the cited references further cannot teach or provide any technical rationale to implement the features of claims 5 and 7, with regard to the authentication credential container being stored at a server and the creation of the user account being performed either automatically or manually by an administrator, at least by virtue of the dependency of claims 5 and 7 from claim 4.

3. Dependent Claim 9

Regarding claim 9, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the authentication information is injected into the separate hardware security device. With regard to this feature, the Office Action (pages 11-12) alleges that Schaeck teaches such a feature in paragraph [0052], lines 11-15. In actuality, paragraph [0052] of Schaeck merely describes how a dynamic runtime integration of web services is made possible by the Schaeck mechanism and may use a composition tool for aggregating new web services. There is nothing in paragraph [0052] of Schaeck that mentions anything regarding injecting authentication information into a separate hardware security device.

4. Dependent Claim 10

Regarding claim 10, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement removing individual user directories for each application of the plurality of the applications accessible by the user. The Office Action (page 12) again points to paragraphs [0043] and [0068] of Schaeck and paragraphs [0108] and [0109] of Delany. The paragraphs of Schaeck cited by the Office Action are just as irrelevant to these features as they are to the other features previously discussed. With regard to the cited portions of Delany, while Delany mentions a deletion function of user management, there is no teaching or technical rationale provided in Delany regarding implementing the specific features of removing *individual user directories for each application of the plurality of the applications accessible by the user*. Thus, any alleged combination of Delany with the other references still would not result in these features being taught or rendered obvious.

5. Dependent Claim 21

With regard to claim 21, Applicant respectfully submits that none of the cited references, either alone or in combination, teaches or provides any technical rationale to implement that the view comprises a list of keys employed by the user, wherein each

entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key. The Office Action (page 13) admits that Schaeck does not teach this feature, but alleges that Delany teaches these features in paragraphs [0361] and [0374]. First, as noted above, Delany does not teach the view recited in independent claim 1 as discussed above, this view being the view referenced in claim 21. Second, the cited sections of Delany teaches that a certificate may include fields specifying a key algorithm, a public key value, and a certificate serial number (see Delany, paragraph [0361]). However, nowhere in Delany is there any teaching of a view that has a list of keys with each entry in the list corresponding to a different key employed by a user. Thus, even though Delany teaches a public key value, a key algorithm, and a certificate serial number, Delany fails to teach or provide any technical rationale to implement these other features of claim 21 which are also not taught or rendered obvious by the other cited references.

6.   Dependent Claim 22

With regard to claim 22, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user. The Office Action (page 13), alleges that these features are taught by Schaeck at paragraphs [0108] and [0109] because Schaeck teaches a user profile. While Schaeck may teach a user profile, this does not teach that the view, which is a consolidated user directory as recited in claim 1, comprises such a profile. Thus, the alleged combination of references still fails to teach or provide any technical rationale to implement the specific features of claim 22.

7.   Dependent Claim 23

Regarding claim 23, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled

application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application. The Office Action (page 14) alleges that these features are taught by Schaeck in paragraphs [0043] and [0068]. Paragraph [0043] merely provides examples of a role specific view of a service. Paragraph [0068] merely describes the defining of separate role views for services. Neither of these portions of Schaeck, or any other portion of Schaeck, teaches or provides any technical rationale to implement the specific features of a list of certificate-enabled applications accessible by a user with entries in the list corresponding to different certificate enabled applications and each entry identifying a user name and a last login attempt of the user. These features are not even really addressed by the Office Action but instead are merely disregarded by pointing to the same general sections of Schaeck previously cited without any analysis as to how they apply to the specific features of the claim. There simply is no teaching in Schaeck, or any of the other cited references, regarding the specific features of claim 23.

8. Dependent Claim 24

Regarding claim 24, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application. Similar to the rejection of claim 23 above, the Office Action (pages 14-15) cites the same sections of Schaeck as allegedly teaching these features but then further states that Delany teaches the last login attempt of the user feature at paragraphs [0428] and [0429]. These paragraphs of Delany generally teach the "logging" of successful and unsuccessful login attempts. However, there is no teaching or technical rationale provided in Delany regarding implementing a view, such as that recited in claim 1 and claim 24 by its dependency, having the entries for each enterprise application and these entries having the user name and last login attempt, as recited in claim 24. The specific arrangement of elements set forth in claim 24 is neither taught nor rendered obvious by the alleged combination of references.

9. Dependent Claim 25

Regarding claim 25, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application. The Office Action (page 15) alleges that these features are taught by Schaeck in paragraphs [0043] and [0068] which have been addressed above. As noted above, these sections only discuss examples of different role views of a service and provide no teaching or technical rationale regarding implementing any list of personal applications, let alone such a list that has entries that correspond to different personal applications with each entry identifying a number of accounts connected to the personal application. There simply is no correlation between the paragraphs of Schaeck and the features of claim 25.

10. Dependent Claim 26

Regarding claim 26, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile. The Office Action (page 15) points to paragraphs [0043], [0044], and [0066] of Schaeck as allegedly teaching these features. Paragraph [0043] provides examples of role based views of a service, paragraph [0044] teaches "user-facing" web applications having user interfaces for communicating with a user, and paragraph [0066] teaches the modification of user profiles. However, nowhere in Schaeck is there any teaching or technical rationale provided regarding implementing a view, such as that recited in claims 1 and 26, having selectable graphical user interface elements to update the profile portion of the view and for invoking a reset of the profile.

11. Dependent Claim 27

Regarding claim 27, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications. Again, the Office Action (page 16) points to paragraphs [0043], [0044], and [0066] as allegedly teaching these features. As noted above with regard to the rejection of claim 26, Schaeck in fact does not teach the specific features of claim 27 in a similar way that Schaeck does not teach the features of claim 26. While Schaeck may generally teach the modification of user profiles, Schaeck provides no teaching or technical rationale provided regarding implementing the specific arrangement of features set forth in claim 27.

III.   Rejection under 35 U.S.C. § 103(a), Claims 16 and 17

The Office Action (pages 16-21) rejects claims 16-17 under 35 U.S.C. §103(a) as being allegedly unpatentable over Schaeck et al. in view of Cotte, and further in view of Yasuda. This rejection is moot with regard to canceled claim 16 and is respectfully traversed with regard to claim 17.

As discussed in the Responses filed April 30, 2008, June 18, 2008 (pages 10-12), and the Appeal Brief filed December 4, 2008, independent Claim 17 recites receiving,*in the data processing system*, in response to a coupling of a separate hardware security device to the data processing system, *credential information for each application of a plurality of applications* that the user uses from the separate hardware security device, *into an authentication credential container associated with the user*. As discussed at length above with regard to claim 1, neither Schaeck, Cotte nor Yasuda, either alone or in combination, teach or provide any technical rationale to implement such features.

As discussed above, in Figure 7 of Schaeck it is clearly shown that the user is presented with available services, the user selects a service, and based on the user's role, portlets associated with the service are selected and combined into an aggregate portal page that is presented to the user. Schaeck provides no teaching or technical rationale

regarding implementing a separate hardware security device, let alone receiving credential information for each application of a plurality of applications that the user uses from the separate hardware security device in response to the separate hardware security device being coupled to a data processing system or receiving such credential information into an authentication credential container associated with the user.

Cotte likewise does not teach or provide any technical rationale regarding implementing these features either, whether Cotte is taken alone or in combination with Schaeck. As discussed above, Cotte teaches that it is possible to access a telecommunications portal in order to retrieve data about different telecommunications web sites residing on that telecommunications portal in total. However, there is nothing in Cotte that teaches or provides any technical rationale to implement the specific features of claim 17 discussed above with regard to Schaeck, i.e. a separate hardware device that is coupled to a data processing system; receiving, *in the data processing system*, in response to a coupling of the separate hardware security device to the data processing system, credential information *for each application of the plurality of applications* that the user uses from the separate hardware security device *into an authentication credential container associated with the user*. Merely providing a telecommunications portal that provides information about telecommunications web sites has nothing to do with identifying a plurality of applications that a user may access from a separate hardware security device in response to such a device being coupled to a data processing system or that a view that is presented is a consolidated user directory that contains user authentication information across the plurality of applications.

Moreover, as discussed above, Yasuda, while teaching a separate hardware security device, i.e. the IC card, only teaches providing a single authentication information for a single application in response to a user selecting an application name from a list. Yasuda does not provide any teaching regarding an authentication credential container in a data processing system or receiving credential information for a plurality of applications from the IC card into the authentication credential container.

Furthermore, none of the cited references teach or provide any technical rationale to display a listing of a plurality of applications accessible by the user *together with any user names and passwords used in connection with the plurality of applications*. To the

contrary, all that Yasuda teaches is displaying a list of application names so that a user can select which application they want to access.

In view of the above, Applicant respectfully submits that neither Schaeck, Cotte, nor Yasuda, either alone or in combination, teaches or provides any technical rationale to implement the features of claim 17. Accordingly, Applicant respectfully requests withdrawal of the rejection of claim 17 under 35 U.S.C. § 103(a).

IV.   Rejection under 35 U.S.C. § 103(a), Claims 18-20

The Office Action rejects claims 18-20 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schaeck, Delany, and Cotte. This rejection is moot in view of the cancelation of these claims.
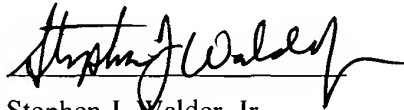
V.   Newly Added Claims 28-31

Claims 28-31 are added to recite computer program product claims corresponding to claims 1, 3, 4, and one or more of claims 21-27. Therefore, claims 28-31 are distinguished over the alleged combination of references for at least similar reasons as set forth above with regard to claims 1, 3, 4, and one or more of claims 21-27. Prompt and favorable consideration of claims 28-31 is respectfully requested.

VI.   Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: July 9, 2009

Stephen J. Walder, Jr.
Reg. No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPLICANT